



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/728,302	12/04/2003	Brian Francis Cox	112025-0530	7927

24267 7590 07/16/2007
CESARI AND MCKENNA, LLP
88 BLACK FALCON AVENUE
BOSTON, MA 02210

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
----------	--------------

2131

MAIL DATE	DELIVERY MODE
-----------	---------------

07/16/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/728,302

Applicant(s)

COX ET AL.

Examiner

Christian La Forgia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 April 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 April 2007 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>6/29/07</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The amendment of 24 April 2007 has been noted and made of record.
2. Claims 1-24 have been presented for examination.

Response to Arguments

3. Applicant's new drawings, filed 24 April 2007, with respect to the drawing objections have been fully considered and are persuasive. The objection of drawings has been withdrawn.
4. The Applicant failed to respond to the Examiner's objection to the Specification, as such it is maintained and repeated below.
5. Applicant's arguments on pages 11 and 12 regarding the 101 rejection filed 24 April 2007 have been fully considered but they are not persuasive.
6. The Applicant argues that claims 18-23 are statutory because the preamble recites that it is an apparatus, yet the Applicant has not shown the structure that the "means for" language is directed toward. Until such a time the Applicant points out the structure to support the "means for" language, the Examiner will continue to interpret the claims as broadly as possible with keeping the specification in mind. Furthermore, the Applicant's failure to particularly point out and distinctly claim the invention may result in rejections under 35 U.S.C. 112, 2nd paragraph in subsequent actions. See MPEP § 2181 (II); see also *In re Donaldson Co.*, 16 F.3d 1189, 1195, 29 USPQ2d 1845, 1850 (Fed. Cir. 1994).
7. Applicant's arguments on pages 12-14 regarding the prior art rejections filed 24 April 2007 have been fully considered but they are not persuasive.
8. Applicant's arguments regarding the prior art rejection fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable

Art Unit: 2131

invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

9. The Examiner disagrees with the Applicant's argument that Roese does not teach partitioning the shared media port into a plurality of logical sub-interfaces, each logical sub-interface dedicated to providing access to a different network or sub-network accessible through the intermediate node. As noted in the previous office action, and on page 13 of the Applicant's response, Roese teaches in paragraph 0012 that the 802.1X standard partitions a single network access point into two logical ports, a logical controlled port and a logical uncontrolled port, thereby teaching at least the partitioning of the shared media port into a plurality of logical sub-interfaces. Roese discloses in paragraphs 0012 and 0015 that communication over the logical uncontrolled port is limited to forwarding authentication messages to the 802.1X Port Access Entity (PAE) while communication over the logical controlled port is granted access to the entire network and its suite of services.

10. Roese, therefore, discloses partitioning the shared media port into a plurality of logical sub-interfaces, each logical sub-interface dedicated to providing access to a different network or sub-network accessible through the intermediate node and the rejection is maintained.

11. The Examiner disagrees with the Applicant's allegation that Roese does not teach determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork. As discussed in the previous Office Action, Roese discloses an authentication decision in figure 3, block 255, and paragraph 0028. This is also discussed in previously cited paragraphs 0012, where Roese states that if a client is

Art Unit: 2131

authenticated, the client can communicate over the logical controlled port while communication is limited to the logical uncontrolled port if the client is not authenticated.

12. There, Roese discloses determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork and the rejection has not been overcome.

13. Applicant's arguments regarding the 103 prior art rejections on pages 14 and 15 fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

14. See further rejections that follow.

Specification

15. The use of the trademark Cisco Systems has been noted on page 13 and 14 in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

16. Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Rejections - 35 USC § 101

17. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

18. Claims 18-23 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. As per claims 18-23, merely claimed as means for where the

Art Unit: 2131

means is implemented in software representing a computer listing *per se*, that is, descriptions or expressions of such a program and that is, descriptive material *per se*, non-functional descriptive material, and is not statutory because it is not a physical “thing” nor a statutory process, as there are not “acts” being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed aspects of the invention which permit the computer program’s functionality to be realized. Since a computer program is merely a set of instructions capable of being executed by a computer, the program itself is not a process, without the computer-readable medium needed to realize the computer program’s functionality. In contrast, a claimed computer-readable medium encoded with a computer program defines structural and functional interrelationships between the computer program and the medium which permit the computer program’s functionality to be realized, and is thus statutory. **Warmerdam**, 33 F.3d at 1361, 31 USPQ2d at 1760. **In re Sarkar**, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106(IV)(B)(1)(a).

19. Page 25, lines 29-30 of the Specification of the instant application describes that the present invention can be implemented as software, thereby rendering the “means for” language in claims 18-23 as computer software. *In re Donaldson Co.*, 16 F.3d 1189, 29 USPQ2d 1845 (Fed. Cir. 1994), decided that

the “broadest reasonable interpretation” that an examiner may give means-plus-function language is that statutorily mandated in paragraph six. Accordingly, the PTO may not disregard the structure disclosed in the specification corresponding to such language when rendering a patentability determination.

See MPEP § 2181 also. Therefore, giving the claims their broadest reasonable interpretation, while keeping the structure disclosed in the specification in my mind, one of ordinary skill in the art would construe claims 18-23 as representing a computer program *per se*.

Claim Rejections - 35 USC § 102

20. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

21. Claims 1-4, 14, 18, and 24 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2004/0158735 to Roese, hereinafter Roese.

22. As per claims 1, 14, 18, and 24, Roese teaches a method, an intermediate node, an apparatus, and a computer-readable medium for implementing port-based network access control at a shared media port in an intermediate node, the shared media port being coupled to a plurality of client nodes, the method comprising:

partitioning the shared media port into a plurality of logical subinterfaces (paragraph [0012], i.e. an authenticator includes one or more sets of controlled and uncontrolled ports), each logical subinterface dedicated to providing access to a different network or subnetwork accessible through the intermediate node (paragraph [0012], i.e. upon authentication, the logical controlled port is enabled and the supplicant is granted access to those network services);

receiving a data packet at the shared media port from a first client node (Figure 3 [block 250], paragraph [0028], i.e. receiving the packets);

associating the received data packet with a first logical subinterface in the plurality of logical subinterfaces (Figure 3 [block 251], paragraph [0028], i.e. inspect the packets for reserved MAC address and 802.1X formats);

determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork (Figure 3 [block 255], paragraph [0028], i.e. rendering an authenticated/not authenticated decision); and

if the first client node is determined to be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork (Figure 3 [block 255], paragraph [0028], i.e. rendering an authenticated/not authenticated decision), forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork (paragraph [0012], i.e. upon authentication, the logical controlled port is enabled and the supplicant is granted access to those network services).

23. Regarding claim 2, Roese teaches performing at least one of dropping the received data packet or reclassifying the received data packet to a different logical subinterface (paragraph [0028], i.e. unrecognized packets are discarded), if the first client node is determined not to be authenticated to communicate over the first logical subinterface's dedicated network or subnetwork (paragraph [0028], i.e. decision rendered that packet is not authenticated).

24. Regarding claim 3, Roese teaches wherein the first logical subinterface's dedicated network or subnetwork is a virtual private network (VPN) (paragraphs [0023], [0025]).

25. Regarding claim 4, Roese teaches wherein a logical subinterface in the plurality of logical subinterfaces is dedicated to providing access to the Internet (Figures 1 [blocks 105a, 105b], 2, paragraph [0023]).

Claim Rejections - 35 USC § 103

26. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

27. Claims 5, 8, 9, 11, 13, 15, 17, 19, and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roese in view of U.S. Patent Application Publication No. 2005/0055570 to Kwan et al., hereinafter Kwan.

28. Regarding claims 5, 17, and 19, Roese teaches wherein the step of determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork further comprises:

parsing a source media access control (MAC) address from the received data packet (Figure 3 [block 251], paragraph [0028], i.e. inspect the packets for reserved MAC address and 802.1X formats);

comparing MAC address and 802.1X formats with stored known Ethernet and authentication packet types (Figure 3 [block 251], paragraph [0028]);

identifying an authentication state stored in the indexed MAC-filter entry (paragraph [0029], i.e. state must be kept on sessions relayed by either MAC address or internal 802.1X protocol); and

determining whether the first client node is authenticated to communicate over the first logical subinterface's dedicated network or subnetwork based on the stored authentication state (Figure 3 [blocks 255], paragraphs [0028]-[0029], i.e. rendering an authenticated/not authenticated decision).

29. Roese does not disclose indexing an entry in a MAC filter to discover authentication state information.

30. Kwan discloses using a MAC filter to control the authentication state of users (paragraphs [0005], [0012], [0013]).

Art Unit: 2131

31. It would have been obvious to one of ordinary skill in the art at the time the invention was made to index an entry in a MAC filter associated with the shared media port based on the value of the parsed source MAC address, and storing the authentication state in the indexed MAC-filter entry, since Kwan states at paragraph [0014] that MAC authentication provides network security in a more efficient manner than conventional solutions.

32. Regarding claims 8 and 21, Roese does not teach wherein the step of associating the received data packet with the first logical subinterface, further comprises locating an entry in a routing table configured to store routing information associated with the received data packet; and associating the received data packet with the first logical subinterface based on the contents of the routing-table entry.

33. Kwan discloses receiving packets and routing the information to the appropriate output port based on information such as the destination address (Figure 2, paragraphs [0033]-[0034]).

34. It would have been obvious to one of ordinary skill in the art at the time the invention was made to locate an entry in a routing table configured to store routing information associated with the received data packet; and associate the received data packet with the first logical subinterface based on the contents of the routing-table entry, since Kwan states at paragraph [0033] that including routing information on a network access device allows a user, such as a system administrator, to reconfigure the network access device and adjust its operating parameters, thereby controlling who can access the data communications network (paragraph [0008]).

Art Unit: 2131

35. Regarding claims 9, 15, and 22, Roese teaches receiving an authentication request from the first client node at the shared media port (Figure 3 [block 250], paragraph [0028], i.e. receiving the packets);

forwarding the received authentication request to an authentication service (Figure 3 [block 252], paragraph [0028]);

receiving a response from the authentication service, the response identifying an authentication state associated with the first client node (Figure 3 [block 256], paragraph [0028]); and

storing the authentication state into which the source MAC address was copied (paragraphs [0028]-[0029]).

36. Roese does not disclose in response to receiving the authentication request, creating a MAC filter associated with the shared media port if the MAC filter has not already been created; copying a source MAC address stored in the received authentication request into an appropriate entry in the MAC filter; and storing the authentication state into the MAC-filter entry.

37. Kwan discloses storing the MAC addresses in a local or global memory (paragraph [0046]), which are used as the control when an authentication request is received (paragraph [0053]).

38. It would have been obvious to one of ordinary skill in the art at the time the invention was made to create a MAC filter in response to receiving the authentication request, copying the source MAC address into the MAC-filter entry, and eventually storing its authentication state, since Kwan states at paragraph [0014] that MAC authentication provides network security in a more efficient manner than conventional solutions.

39. With regards to claims 11 and 23, Roesse teaches wherein the received authentication request is an 802.1X authentication request (paragraph [0028], i.e. 802.1X EAP (Extensible Authentication Protocol)).

40. With regards to claim 13, Roesse teaches sending an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node's authentication state changes from an authenticated state to an unauthenticated or unknown state (paragraph [0029], i.e. tracking state changes via a tracking function).

41. Claims 6 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roesse in view of Kwan as applied to claim 5 above, and further in view of U.S. Patent Application Publication No. 2005/0177865 to Ng et al., hereinafter Ng.

42. With regards to claim 6, Roesse and Kwan do not teach wherein the MAC filter is organized as a hash table.

43. Ng discloses wherein the state information has been stored using a hash function (paragraph [0080]).

44. It would have been obvious to one of ordinary skill in the art at the time the invention was made to organize the MAC filter as a hash table, since one of ordinary skill in the art would recognize that the MAC addresses were being used as authentication means it would be necessary to store the address in a protected format, similar to how Unix systems store user

Art Unit: 2131

passwords in a hashed file, to prevent unauthorized users from acquiring the MAC addresses if the intermediate node was ever compromised.

45. With regards to claim 10, Roese and Kwan do not teach indexing an entry in the MAC filter based on the result of applying a hash function to the source MAC address; and storing the source MAC address at the indexed MAC-filter entry.

46. Ng discloses hashing local node information along with the state information for authentication purposes (paragraph [0080]).

47. It would have been obvious to one of ordinary skill in the art at the time the invention was made to index an entry in the MAC filter based on the result of applying a hash function to the source MAC address and store the source MAC address at the indexed MAC-filter entry, since one of ordinary skill in the art would recognize that the MAC addresses were being used as authentication means it would be necessary to store the address in a protected format, similar to how Unix systems store user passwords in a hashed file, to prevent unauthorized users from acquiring the MAC addresses if the intermediate node was ever compromised.

48. Claims 7, 16, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roese in view of U.S. Patent Application No. 2004/0208151 to Haverinen et al., hereinafter Haverinen.

49. Regarding claims 7, 16, and 20, Roese does not teach parsing a destination Internet Protocol (IP) address from the received data packet; comparing the parsed destination IP address to one or more IP addresses stored in an IP filter associated with the shared media port; and if the

Art Unit: 2131

parsed destination IP address matches an IP address stored in the IP filter, forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork, even if the first client node is determined not to be authenticated to communicate over that network or subnetwork.

50. Haverinen teaches parsing a destination Internet Protocol (IP) address from the received data packet (Figure 1 [blocks 104], paragraph [0029], i.e. receive IP address);

comparing the parsed destination IP address to one or more IP addresses stored in an IP filter associated with the shared media port (Figure 1 [block 105], paragraph [0029], i.e. IP authentication protocol); and

if the parsed destination IP address matches an IP address stored in the IP filter, forwarding the received data packet over the first logical subinterface's dedicated network or subnetwork (paragraph [0029], i.e. successful IP authentication protocol allows access controller to relay data packets of terminal device), even if the first client node is determined not to be authenticated to communicate over that network or subnetwork (Figure 1 [block 102], i.e. no IEEE 802.1X authentication).

51. It would have been obvious to one of ordinary skill in the art at the time the invention was made to perform an open systems authentication protocol, since Haverinen states at paragraph [0004] that using an open systems authentication protocol, specifically one focused on the third layer of the OSI model, allows wireless users to authenticate and access network resources, thereby allowing users the freedom to access network resource whenever and where ever they would like.

52. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Roese in view of Kwan as applied to claim 9 above, and further in view of U.S. Patent No. 6,891,819 to Inoue et al., hereinafter Inoue.

53. With regards to claim 12, Roese and Kwan do not teach sending an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node fails to authenticate at the shared media port a predetermined number of times.

54. Inoue discloses tracking the number of times a user has failed authentication and providing an indication that said account has failed authentication a predetermined number of times (Figures 12-14, 18 and 19, column 12, lines 45-67, column 13, lines 22-46, column 17, lines 53-59).

55. It would have been obvious to one of ordinary skill in the art at the time the invention was made to send an alarm message over the first logical subinterface's dedicated network or subnetwork after the first client node fails to authenticate at the shared media port a predetermined number of times, since Inoue states at column 3, lines 1-6 that tracking the number an authentication fails helps to prevent the improper acquisition of user or network information since reaching the threshold of improper authorization attempts is a clear indicator that the user account or mobile system has been compromised.

Conclusion

56. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

57. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

Art Unit: 2131

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

58. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

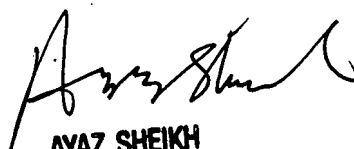
59. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

60. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

Art Unit: 2131

clf



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100